Threshold Circuit Lower Bounds on Cryptographic Functions

Eike Kiltz

Fakultät für Mathematik,
Lehrstuhl Mathematik & Informatik,
Ruhr-Universität Bochum,
44780 Bochum, Germany.

Hans Ulrich Simon

Fakultät für Mathematik,
Lehrstuhl Mathematik & Informatik,
Ruhr-Universität Bochum,
44780 Bochum, Germany

Abstract

In this work, we are interested in non-trivial upper bounds on the spectral norm of binary matrices M from $\{-1,1\}^{N \times N}$. It is known that the distributed Boolean function represented by M is hard to compute in various restricted models of computation if the spectral norm is bounded from above by $N^{1-\varepsilon}$, where $\varepsilon > 0$ denotes a fixed constant. For instance, the size of a two-layer threshold circuit (with polynomially bounded weights for the gates in the hidden layer, but unbounded weights for the output gate) grows exponentially fast with $n := \log N$. We prove sufficient conditions on M that imply small spectral norms (and thus high computational complexity in restricted models). Our general results cover specific cases, where the matrix M represents a bit (the least significant bit or other fixed bits) of fundamental functions. Functions like the discrete multiplication and division, as well as cryptographic functions such as the Diffie-Hellman function [5] and the decryption functions of the Pointcheval [22] and the ElGamal [9] cryptosystems can be addressed by our technique. In order to obtain our results, we make a detour on exponential sums and on spectral norms of matrices with complex entries. This method might be considered interesting in its own right.

Key words: Threshold circuits, exponential sums, Spectral Norm

Email addresses: `kiltz@lmi.ruhr-uni-bochum.de` (Eike Kiltz), `simon@lmi.ruhr-uni-bochum.de` (Hans Ulrich Simon).

1 Introduction

In this paper, we apply a powerful technique by Forster [6] for proving lower bounds on the computational resources needed to compute distributed Boolean functions, i.e., functions of the form $f_n : \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}$. Forster associates the matrix $F_n \in \{-1,1\}^{2^n \times 2^n}$ given by $F_n(x,y) = (-1)^{f_n(x,y)}$ with each such function. His key result states that the smallest rank of any matrix that can be obtained from F_n by sign-preserving changes of its entries (replacing -1's by negative and $+1$'s by positive real numbers) is at least $2^n / \|F_n\|_2$, where $\|\cdot\|_2$ denotes the spectral norm (also called operator norm) of a matrix. An equivalent way to state this result is saying that the probabilistic communication complexity of f_n in the unbounded error model of Paturi and Simon [21] is at least $n - \log \|F_n\|_2$. As exploited by Forster himself [6], this leads to a lower bound of $n/2$ on the probabilistic communication complexity (in the unbounded error model) of the "inner product modulo 2" function (which induces the ± 1-valued Hadamard matrix of spectral norm $2^{n/2}$). As explained in [7], there are other striking consequences of Forster's result. For instance, a two-layer linear threshold circuit with unbounded weights on the top-layer (but bounded weights on the bottom-layer) cannot compute the "inner product modulo 2" function unless there are exponentially many gates. Since Forster's key result is stated in terms of the spectral norm, similar remarks apply to distributed Boolean function f_n whose corresponding matrix F_n has a "sufficiently small" spectral norm. In particular, it holds for any matrix with (almost) orthogonal rows or columns. Apart from the orthogonality argument, however, there don't seem to be so many techniques available which lead to sharp enough upper bounds on spectral norms in a convenient fashion for a wide range of applications. Without such techniques, the powerful result of Forster cannot be exploited to full extent.

In this paper, we demonstrate how "exponential sums" can be used to obtain upper bounds on the spectral norm of a ± 1-valued matrix. We make a detour on (suitably defined) matrices over the complex numbers. Bounds on exponential sums from [3,8,28] (see also [26]) are used to obtain the bounds on the spectral norms of these matrices.

Inspired from investigations in cryptography concerning bit-security, we are particularly interested in matrices of the form $B \circ H$, where $H(x,y)$ is a function with range $\mathbb{Z}_N$ (integers modulo N) and B is a ± 1-valued predicate defined on $\mathbb{Z}_N$ (revealing one bit of information over the given integer modulo N). Rather surprisingly, upper bounds on the spectral norm of $B \circ H$ can be proven under quite general conditions:

- H should be a close enough relative of either discrete multiplication (modulo N) or of discrete exponentiation (modulo N).

- B should be "balanced" in the sense that it is not significantly biased towards either -1 or $+1$ and satisfies an additional (more technical) balance-condition.

We show that a surprisingly wide spectrum of functions (including some popular cryptographic function families) and binary predicates (including the bits of the binary encoding except for the most significant-ones) fits into this framework. As an immediate consequence of these results, the (at the time being) strongest known lower bounds on the size of bounded-depth linear threshold circuits actually apply to a surprisingly broad family of quite natural families of Boolean functions.

For a special case of functions B and H, an upper bound on the spectral norm of $B \circ H$ can already be achieved with results known in the literature. Consider the matrix representing the least significant bit of the Diffie-Hellman function [5] modulo a prime number N. Shparlinski [25] could show that a related measure (the discrepancy [24]) of this matrix is upper bounded by $N^{-1/24+o(1)}$. Applying a general bound from Shaltiel [24], we infer that the spectral norm of $B \circ H$ is bounded from above by $N^{71/72+o(1)}$. We can improve on Shparlinski's result in several ways. By a more refined analysis we can "bypass" Shaltiel's general bound [24] improving the constant from 71/72 to 23/24. Furthermore, we build a whole theory around this result leading to upper bounds on the spectral norm of more general matrices of the form $B \circ H$. Since we deal with the algebraic object "spectral norm", our techniques have a more algebraic touch than the ones used in [25]. We would like to refer the reader to the textbook of Shparlinski [26] for an overview on the application of analytic number theory techniques in complexity theory.

The paper is organized as follows. In Section 2 we will remind the reader of some definitions and facts about linear threshold circuits and review a lower bound method from [7]. In Section 3 we will present our main results that will be proven in Section 4. Some parts of the proof are somewhat tedious and therefore postponed to Appendix A. In Section 5 we will mention some applications of our general results. Finally, in Section 6 we will make some remarks and show possible extensions.

This paper contains extracts from the first authors PhD thesis [15]. It combines and extends the two papers by Kiltz [14] and Kiltz and Simon [16].

2 Linear Threshold Circuits and a Lower Bound Technique

We will consider Boolean functions on $2n$ variables

$$f_n : \{0,1\}^n \times \{0,1\}^n \to \{0,1\} \ .$$

They can be identified in a natural way by a ± 1-valued $2^n \times 2^n$ matrix. For an integer N with $2^{n-1} < N \leq 2^n$, we identify the elements $x \in \mathbb{Z}_N$ with $x \in \{0,1\}^n$. We make the following definition:

Definition 2.1 *Let $2^{n-1} < N \leq 2^n$. We say a matrix $A \in \{-1,1\}^{N\times N}$* represents a Boolean function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ *on* $\{0,\ldots,N-1\} \times \{0,\ldots,N-1\}$*, if $A_{x,y} = (-1)^{f(x,y)}$ for all $x, y \in \{0,\ldots,N-1\}$.*

We will be interested in circuits over the (complete) basis consisting of *linear threshold functions*. A linear threshold function $G_\alpha : \{0,1\}^n \to \{0,1\}$ with respect to the integer weights $\alpha_1,\ldots,\alpha_n$ and threshold α_0 is the function defined as $G_\alpha(x_1,\ldots,x_n) = \mathrm{sign}(\sum_{i=1}^n \alpha_i x_i - \alpha_0)$, where the (0,1-valued) signum function $\mathrm{sign} : \mathbb{R} \to \{0,1\}$ is given by $\mathrm{sign}(x) = 1$ for $x \geq 0$, and $\mathrm{sign}(x) = 0$ otherwise. For a threshold gate, the *weight* is the maximum of the absolute values of all integer weights of the gate. There is a difference when considering threshold functions of bounded and unbounded weight. We are interested in the following two complexity classes:

- LT_k: all $0,1$-valued functions computable by threshold circuits of polynomial size, depth k and unbounded integer weights.
- TC_k: all $0,1$-valued functions computable by threshold circuits of polynomial size, depth k and polynomially bounded integer weights.
- $\check{\mathrm{LT}}_k$: all $0,1$-valued functions computable by threshold circuits of polynomial size, depth k, where the bottom layer has polynomially bounded integer weights and the remaining gates have unbounded integer weights.

These classes form the following hierarchy [10,12,18] which we zoom in for the cases $k = 2,3$:

$$\ldots \mathrm{TC}_2 \subsetneq \check{\mathrm{LT}}_2 \subseteq \mathrm{LT}_2 \subseteq \mathrm{TC}_3 \subseteq \ldots \tag{1}$$

A few comments are in place here:

- For the "inner product modulo two" function, IP, it was shown in [7] that $\mathrm{IP} \notin \check{\mathrm{LT}}_2$ and hence (since $\mathrm{IP} \in \mathrm{TC}_3$ [12]) we have $\check{\mathrm{LT}}_2 \subsetneq \mathrm{TC}_3$. In this paper we will present new examples of binary functions in $\mathrm{TC}_3 \setminus \check{\mathrm{LT}}_2$:
- With methods from [2] and [10] it can be shown that the function $p(x,y) = \mathrm{sign}\left(1 + 2\sum_{i=0}^{n-1}\sum_{j=0}^{2n-1} 2^i y_j (x_{i,2j} + x_{i,2j+1})\right)$ (introduced in [10]) is contained in $\check{\mathrm{LT}}_2 \setminus \mathrm{TC}_2$.

As we will explain below, there are good techniques for showing that a function is not contained in $\check{\mathrm{LT}}_2$. The question whether LT_2 is different from higher levels of the hierarchy (or whether it contains all of NP) is still open. So, the frontier between solved and unsolved problems concerning threshold circuits lies in the region of depth 2.

The so-called spectral norm of a matrix with real or complex entries plays a central role in our paper:

Definition 2.2 *The* spectral norm *of $A \in \mathbb{R}^{N_1 \times N_2}$ is defined as follows:*

$$\|A\|_2 = \max_{\substack{u \in \mathbb{R}^{N_1}, v \in \mathbb{R}^{N_2} \\ \|u\|_2 = \|v\|_2 = 1}} \left| u^\top A v \right| \tag{2}$$

Here, the maximum ranges over vectors with real components. The analogous definition is used for matrices from $\mathbb{C}^{N_1 \times N_2}$. (Clearly, the maximum then ranges over vectors with complex components.)

The *Frobenius norm* of a matrix $A \in \mathbb{C}^{N_1 \times N_2}$ is defined as

$$\|A\|_F := \left(\sum_{j=0}^{N_1-1} \sum_{k=0}^{N_2-1} A_{j,k}^2 \right)^{1/2} .$$

Note that $\|A\|_F = \sqrt{N_1 N_2}$ for each $A \in \{-1,1\}^{N_1 \times N_2}$. We have the following relation between the spectral norm and the Frobenius norm for each matrix $A \in \mathbb{C}^{N_1 \times N_2}$ [13]:

$$\frac{\|A\|_F}{\sqrt{\mathrm{rank}(A)}} \le \|A\|_2 \le \|A\|_F \ . \tag{3}$$

As an immediate consequence of (3) we get the following inequalities for square matrices with entries of absolute value 1:

$$N^{1/2} \le \|A\|_2 \le N \ . \tag{4}$$

Furthermore, $\|A\|_2 = N^{1/2}$ iff A is orthogonal and $\|A\|_2 = N$ iff $\mathrm{rank}(A) = 1$ [13].

To simplify notation we will not distinguish between a vector $x \in \{0,1\}^n$ and the integer $x = \sum_{i=0}^{n-1} x_i 2^i$.

Now we review a result from [7] (based on a result from Forster [6]) stating that a function whose corresponding spectral norm is upper bounded by $N^{1-\varepsilon}$ (for a constant $\varepsilon > 0$), cannot be contained in the complexity class $\check{\mathrm{LT}}_2$. We present it in a slightly modified version.

Theorem 2.3 *Let (f_n) be a family of distributed Boolean functions $f_n : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$. Suppose (f_n) is computed by depth-2 threshold circuits (C_n)*

in which the top gate is a linear threshold gate using unrestricted *weights and the bottom level has linear threshold gates using weights whose absolute value is upper bounded by a polynomial in n. Assume* $\|A_N\|_2 = O(N^{1-\varepsilon})$ *for a constant* $0 < \varepsilon \leq 1/2$*, where* A_N *is the matrix representing* f_n *on* $\{0, \ldots, N-1\} \times \{0, \ldots, N-1\}$ $(2^n \leq N < 2^{n+1})$*. Then the number of threshold gates that is necessary to compute* (f_n) *is lower bounded by* $2^{\varepsilon n - O(\log n)} = N^{\varepsilon - o(1)}$.

By means of Theorem 2.3, membership in $\check{\mathrm{LT}}_2$ can be ruled out in a convenient manner. It gives nowadays the largest lower bounds for depth-2 threshold circuits.

3 Upper Bounds on the Spectral Norm

Let $\mathcal{X}$ and $\mathcal{Y}$ be finite sets. In this Section, we identify functions of the form $H : \mathcal{X} \times \mathcal{Y} \to \mathcal{Z}$ with matrices from $\mathcal{Z}^{\mathcal{X} \times \mathcal{Y}}$. Similarly, functions of the form $K : \mathcal{Z} \to \mathcal{K}$ are viewed as (column) vectors from $\mathcal{K}^{\mathcal{Z}}$. Note that the composition $K \circ H : \mathcal{X} \times \mathcal{Y} \to \mathcal{K}$ can then be identified with a matrix from $\mathcal{K}^{\mathcal{X} \times \mathcal{Y}}$. We are mainly interested in the following situation:

- $\mathcal{X} = \mathcal{Y} = \{0, \ldots, T-1\}$ (or $\mathcal{X} = \mathcal{Y} = \mathbb{Z}_T$) [1], and $\mathcal{Z} = \mathbb{Z}_N$ (where, in general, N may differ from T).
- In the role of K, we consider functions $B : \mathbb{Z}_N \to \{-1, 1\}$ and the complex functions $E_a : \mathbb{Z}_N \to \mathbb{C}$ defined as $E_a(z) = e^{\frac{2\pi i a z}{N}}$ for each $a \in \mathbb{Z}_N$.

Functions E_a are used as a mathematical tool within the analysis of the computational complexity of $B \circ H$. We pursue the strategy to bound the spectral norm of $B \circ H$ in terms of the spectral norm of $E_a \circ H$ (and some other terms). The hope is that "good" upper bounds on the spectral norm of $E_a \circ H$ are known (or easy to compute) and that they can be converted into "good" upper bounds on the spectral norm of $B \circ H$.

This section is organized as follows: In Subsection 3.1 we introduce the notion of functions H having *multiplicative* and *exponential structure*. The bounds on the spectral norm of $B \circ H$ will also depend on two parameters (refered to as balance terms) associated with the Boolean function B. These parameters are introduced in Subsection 3.2. The main results of this work are stated in Subsection 3.3.

[1] We prefer the notation $\mathbb{Z}_T$ (as opposed to $\{0, \ldots, T-1\}$) whenever we want to underline the algebraic structure.

3.1 Functions with Multiplicative and Exponential Structure

Let $M : \mathbb{Z}_N \times \mathbb{Z}_N \to \mathbb{Z}_N$ be the function that satisfies $M(x, y) = xy$ (multiplication in $\mathbb{Z}_N$). We want to exploit the fact that some (cryptographic) functions are close relatives of M. The general concept of a "multiplicative structure" is captured in the following definition:

Definition 3.1 *Let $\mathcal{X}$ and $\mathcal{Y}$ be two subsets of $\{0, \ldots, N-1\}$. We say $H : \{0, \ldots, N-1\} \times \{0, \ldots, N-1\} \to \mathbb{Z}_N$ has a* multiplicative structure on subdomain $\mathcal{X} \times \mathcal{Y} \subseteq \{0, \ldots, N-1\} \times \{0, \ldots, N-1\}$ *if there exist injective functions $\sigma : \mathcal{X} \to \mathbb{Z}_N$ and $\tau : \mathcal{Y} \to \mathbb{Z}_N$ such that*

$$H(x, y) = M_{\sigma,\tau}(x, y) := \sigma(x) \cdot \tau(y)$$

for all $x \in \mathcal{X}$ and $y \in \mathcal{Y}$, where $H(x, y)$ may take arbitrary values outside $\mathcal{X} \times \mathcal{Y}$.

Let $D : \mathbb{Z}_T \times \mathbb{Z}_T \to \mathbb{Z}_N$ be the function that satisfies $D(x, y) = g^{xy}$ (exponentiation in $\mathbb{Z}_N$), where $g \in \mathbb{Z}_N^*$ is an element of order T. Again we want to exploit the fact that some functions are close relatives to D. We define the general concept of an "exponential structure" as follows:

Definition 3.2 *Let $g \in \mathbb{Z}_N^*$ be an element of order T. We say $H : \{0, \ldots, T-1\} \times \{0, \ldots, T-1\} \to \mathbb{Z}_N$ has an* exponential structure on subdomain $\mathcal{X} \times \mathcal{Y} \subseteq \{0, \ldots, T-1\} \times \{0, \ldots, T-1\}$ with respect to g *if there exist injective functions $\sigma : \mathcal{X} \to \mathbb{Z}_T$ and $\tau : \mathcal{Y} \to \mathbb{Z}_T$ such that*

$$H(x, y) = D_{\sigma,\tau}(x, y) := g^{\sigma(x)\tau(y)} \quad ,$$

for all $x \in \mathcal{X}$ and $y \in \mathcal{Y}$, where $H(x, y)$ may take arbitrary values outside $\mathcal{X} \times \mathcal{Y}$.

An analogous definition can be made for functions $H : \{1, \ldots, T\} \times \{1, \ldots, T\} \to \mathbb{Z}_N$. Examples of functions H with multiplicative or exponential structure are given in Section 5.

3.2 The Balance Terms

Given a Boolean predicate B, we will introduce two terms, $EXP_B(N, d)$ and $\mathrm{bias}_B(N)$, that will render themselves useful in our analysis. We refer to the terms $\mathrm{bias}_B(N)$ and $EXP_B(N, d)$ as the *balance terms associated with B*. In particular, we are interested in non-trivial upper bounds on the values $EXP_B(N, d)$ and $\mathrm{bias}_B(N)$. As we will see later, in order to obtain good bounds on the spectral norm of $B \circ H$ using our technique, "good bounds" on $EXP_B(N,d)$ and $\mathrm{bias}_B(N)$ will be a necessary condition.

As mentioned above already, the function $E_a^N : \mathbb{Z}_N \to \mathbb{C}$ is defined as

$$E_a^N(z) = e^{\frac{2\pi i a z}{N}} = \cos\frac{2\pi a z}{N} + i \cdot \sin\frac{2\pi a z}{N} \tag{5}$$

for each $a \in \mathbb{Z}_N$. In the sequel we drop superscript N when it is obvious from context.

For a divisor $d < N$ of N, define

$$EXP_B(N,d) := \frac{d}{N} \sum_{a \in \mathbb{Z}_{N/d}^*} |\langle B, E_{ad}\rangle| = \frac{d}{N} \sum_{a \in \mathbb{Z}_{N/d}^*} \left| \sum_{x \in \mathbb{Z}_N} B(x) E_{ad}(x) \right| \ . \tag{6}$$

We would like to stress that $\langle B, E_{ad}\rangle = \sum_{x \in \mathbb{Z}_N} B(x)E_{ad}(x)$ denotes the inner product of B and E_{ad} in $\mathbb{C}$ when we view the functions $B : \mathbb{Z}_N \to \{-1,1\}$ and $E_{ad} : \mathbb{Z}_N \to \mathbb{C}$ as vectors with complex entries. Since $|E_{ad}(x)| = 1$, $EXP_B(N,d)$ is trivially upper bounded by N. We call B *smooth* if it satisfies

$$EXP_B(N,d) = N^{o(1)} \ , \tag{7}$$

for all divisors $d < N$ of N.[2] The *bias* of a binary function $B : \mathbb{Z}_N \to \{-1,1\}$ is given by

$$\mathrm{bias}_B(N) := \left| \sum_{z \in \mathbb{Z}_N} B(z) \right| \in \{0, \ldots, N\} \ . \tag{8}$$

The bias measures the degree of "balance" between negative and positive entries in vector B (where value 0 reflects perfect balance). Function $B : \mathbb{Z}_N \to \{-1,1\}$ is called *unbiased* if

$$\mathrm{bias}_B(N) = N^{o(1)} \ .$$

Functions that are at the same time unbiased and smooth will play a central role in our results.

Definition 3.3 *We call a binary function $B : \mathbb{Z}_N \to \{-1,1\}$* balanced *if it is unbiased (i.e., $\mathrm{bias}_B(N) = N^{o(1)}$) and smooth (i.e., $EXP_B(N,d) = N^{o(1)}$).*

[2] More formally, $B = B_N$ is a family of Boolean functions, where N ranges over (a subset of) the natural numbers $\mathbb{N}$.

We are now ready to present the main results of this paper.

Theorem 3.4 *Let B be a balanced binary function. Let H be a function with a multiplicative structure on subdomain $\mathcal{X}\times\mathcal{Y}$ of $\{0,\ldots,N{-}1\}\times\{0,\ldots,N{-}1\}$. Assume that $N-|\mathcal{X}|=O(N^\alpha)$ and $N-|\mathcal{Y}|=O(N^\alpha)$ for some fixed constant $0\le\alpha<1$. Then, the spectral norm of matrix $B\circ H$ is bounded from above by*

$$\|B\circ H\|_2 = \begin{cases} N^{1/2+o(1)} & : \quad \alpha=0 \\ O(N^{(1+\alpha)/2}) & : \quad \alpha\neq 0. \end{cases}$$

Theorem 3.5 *For integers N, let T be the order of an element $g\in\mathbb{Z}_N^*$. Let B be a balanced binary function. Let $H:\{0,\ldots,T{-}1\}\times\{0,\ldots,T{-}1\}\to\mathbb{Z}_N$ be a function with an exponential structure on subdomain $\mathcal{X}\times\mathcal{Y}$ of $\{0,\ldots,T{-}1\}\times\{0,\ldots,T{-}1\}$ with respect to g. Assume that $T-|\mathcal{X}|=O(T^{5/16}N^{5/8})$ and $T-|\mathcal{Y}|=O(T^{5/16}N^{5/8})$. Then, the spectral norm of matrix $B\circ H$ is bounded from above by*

$$\|B\circ H\|_2 = T^{21/32}N^{5/16+o(1)} \quad .$$

Note that $B\circ H$ is a $T\times T$ matrix and hence the theorem gives a nontrivial bound on $\|B\circ H\|_2$ (a bound of order $T^{1-\varepsilon}$, $\varepsilon>0$) for elements g of order $T>N^{10/11+\delta}$ for any positive constant δ.

Theorem 3.6 *For primes N let T be the order of an element $g\in\mathbb{Z}_N^*$. Let B be a balanced binary function. Let $H:\{0,\ldots,T{-}1\}\times\{0,\ldots,T{-}1\}\to\mathbb{Z}_N$ be a function with an exponential structure on subdomain $\mathcal{X}\times\mathcal{Y}$ of $\{0,\ldots,T{-}1\}\times\{0,\ldots,T{-}1\}$ with respect to g. Assume that $T-|\mathcal{X}|=O(T^{2/3}N^{1/4})$ and $T-|\mathcal{Y}|=O(T^{2/3}N^{1/4})$. Then, the spectral norm of matrix $B\circ H$ is bounded from above by*

$$\|B\circ H\|_2 = T^{5/6}N^{1/8+o(1)} \quad .$$

This gives a nontrivial bound on $\|B\circ H\|_2$ for elements g of order $T>N^{3/4+\delta}$ for any positive constant δ.

The proof of the last three Theorems is given in Section 4. The next theorem shows that many natural binary functions are balanced.

Theorem 3.7 *The following binary functions $B:\mathbb{Z}_N\to\{-1,1\}$ are balanced:*

- *Let B_k denote the k-th least significant bit of (the binary representation of) $z\in\mathbb{Z}_N$. Assume that k is either constant or (as a function in N) satisfies*

$k(N) = o(\log N)$.[3] *Then B_k is balanced.*
- *Let B denote any unbiased and strongly semilinear function of length k (see Definition A.1). Assume that k is either constant or (as a function in N) satisfies $k(N) = N^{o(1)}$. Then B is balanced.*

Since the proof of the last theorem is a little bit technical, we decided to postpone it to Appendix A.

One may combine now any of these balanced binary functions with Theorem 3.4, Theorem 3.5, or Theorem 3.6 to get the result that the spectral norm of *concrete binary functions* is at most $T^{1-\varepsilon}$ for a constant $\varepsilon > 0$. As mentioned before, we may now apply the lower bound machinery from Theorem 2.3 to get complexity theoretic lower bounds.

4 The Proof

This section is devoted to the proofs of the Theorems 3.4, 3.5, and 3.6. The roadmap is as follows. First, in Subsection 4.1, we present a general "Splitting Lemma" that breaks the spectral norm of $B \circ H$ into two components. The first component will only depend on the balance terms associated with B. Providing upper bounds on the balance terms for concrete Boolean functions B will be subject of Appendix A. The second component will only depend on the matrix H and spectral norms of complex *auxiliary matrices* $E_a \circ H$ will appear (thereby putting *exponential sums* into play). In Subsection 4.2 we will upper bound the spectral norm of these auxiliary matrices for the concrete functions $M(x, y) = xy$ and $D(x, y) = g^{xy}$ in the role of H. Finally in Subsection 4.3, our main theorems from Section 3.3 about functions with muliplicative (Theorem 3.4) and exponential structure (Theorems 3.5 and 3.6), resp., are proven.

Before we go on, we collect some useful properties of the function E_a (as defined in Eq. (5)). Clearly, the following rules are valid:

$$
\begin{aligned}
E_x(a) &= E_a(x) = E_a(1)^x && (9)\\
|E_a(x)| &= 1 && (10)\\
E_a(x+y) &= E_a(x) \cdot E_a(y) && (11)\\
\overline{E_a(x)} &= E_{-a}(x) && (12)\\
\sum_{a \in \mathbb{Z}_N} E_{-a}(y) &= \sum_{a \in \mathbb{Z}_N} E_a(y) && (13)
\end{aligned}
$$

[3] This rules out the possibility to select bits of high significance (not to speak of the most significant bit).

Since $E_a(x) = E_a(1)^x$, we get for every $a \in \mathbb{Z}_N \setminus \{0\}$:

$$\sum_{x=0}^{P-1} E_a(x) = \frac{E_a(P) - 1}{E_a(1) - 1} \quad . \tag{14}$$

In combination with $E_a(N) = E_a(0) = 1$, this yields

$$\frac{1}{N} \sum_{z \in \mathbb{Z}_N} E_z(a) = \frac{1}{N} \sum_{z \in \mathbb{Z}_N} E_a(z) = \begin{cases} 0 \text{ if } a \neq 0, \\ 1 \text{ if } a = 0. \end{cases} \tag{15}$$

We can immediately infer the following identity, which holds for each function $B : \mathbb{Z}_N \to \{-1, 1\}$:

$$B(z_0) = \frac{1}{N} \sum_{z \in \mathbb{Z}_N} \left(B(z) \sum_{a \in \mathbb{Z}_N} E_a(z_0 - z) \right) \quad . \tag{16}$$

4.1 The Splitting Lemma

For $T \leq N$, let $H : \mathbb{Z}_T \times \mathbb{Z}_T \to \mathbb{Z}_N$ be a matrix and let $B : \mathbb{Z}_N \to \{-1, 1\}$ be a binary function. In this subsection, we present the central idea of bounding the spectral norm of matrices of the form $B \circ H$. We will split it into two independent components, one only depending on the binary function B, the other one only depending on the matrix H.

The main result in this subsection reads as follows:

Lemma 4.1 $\|B \circ H\|_2 \leq bias_B(N) + \frac{1}{N} \cdot \sum_{a=1}^{N-1} |\langle B, E_{-a} \rangle| \, \|E_a \circ H\|_2$.

PROOF. Choose $u, v \in \mathbb{R}^T$ such that $\|u\|_2 = \|v\|_2 = 1$ and $\|B \circ H\|_2 = |u^\top (B \circ H) v|$. We obtain

$$\begin{aligned} |u^\top (B \circ H) v| &= \left| \sum_{x \in \mathbb{Z}_T} \sum_{y \in \mathbb{Z}_T} u_x v_y B(H(x,y)) \right| \\ &\overset{(16)}{=} \frac{1}{N} \left| \sum_{x \in \mathbb{Z}_T} \sum_{y \in \mathbb{Z}_T} u_x v_y \sum_{z \in \mathbb{Z}_N} \sum_{a \in \mathbb{Z}_N} B(z) E_a(H(x,y) - z) \right| \\ &\overset{(11)}{=} \frac{1}{N} \left| \sum_{a \in \mathbb{Z}_N} \sum_{z \in \mathbb{Z}_N} B(z) E_{-a}(z) \sum_{x \in \mathbb{Z}_T} \sum_{y \in \mathbb{Z}_T} u_x v_y E_a(H(x,y)) \right| \\ &\leq \frac{1}{N} \sum_{a \in \mathbb{Z}_N} S(a) \quad , \end{aligned}$$

where $S(a)$ is given by

$$\begin{aligned} S(a) &= \left| \sum_{z \in \mathbb{Z}_N} B(z) E_{-a}(z) \sum_{x \in \mathbb{Z}_T} \sum_{y \in \mathbb{Z}_T} u_x v_y E_a(H(x,y)) \right| \\ &\le |\langle B, E_{-a} \rangle| \cdot |u^\top (E_a \circ H) v| \\ &\le |\langle B, E_{-a} \rangle| \cdot \| E_a \circ H \|_2 \ . \end{aligned}$$

The proof is completed by discussing the case $a = 0$ separately. Since $E_0(z) = 1$ for each $z \in \mathbb{Z}_N$ and $T \le N$, we get

$$\frac{1}{N} S(0) \overset{(4)}{\le} \frac{T}{N} \left| \sum_{z \in \mathbb{Z}_N} B(z) \right| \le \left| \sum_{z \in \mathbb{Z}_N} B(z) \right| = \mathrm{bias}_B(N) \ .$$

□

The Splitting Lemma 4.1 shows that for computing an upper bound on the spectral norm $\|B \circ H\|_2$ it is sufficient to give an upper bound on $\langle B, E_{-a} \rangle$ and on the spectral norm $\|E_a \circ H\|_2$. Note that the matrix $E_a \circ H$ is a complex matrix from $\mathbb{C}^{T \times T}$.

We would like to have a bound on $\|E_a \circ H\|_2$ for concrete functions H that holds uniformly for all $a \in \mathbb{Z}_N \setminus \{0\}$. Unfortunately we are not able to do so and, as it will turn out, our bound on $\|E_a \circ H\|_2$ will also depend on the value $d = \gcd(a, N)$. To this end we cut the set $\mathbb{Z}_N$ into $\tau(N)$ different slices, where $\tau(N)$ is the number of divisors of N. The d-th slice contains all $a \in \mathbb{Z}_N$ such that $\gcd(a, N) = d$. These are precisely the elements of the form ad for $a \in \mathbb{Z}_N^*$. We make the following definition:

$$U_H(N) = \max_{d : d | N, d < N} \frac{1}{d} \max_{a \in \mathbb{Z}_{N/d}^*} \|E_{ad} \circ H\|_2 \ . \tag{17}$$

We briefly note the well-known fact [23] that

$$\tau(N) = 2^{(1+o(1)) \frac{\ln N}{\ln \ln N}} = N^{o(1)} \ . \tag{18}$$

This leads to the following

Corollary 4.2 *For smooth binary functions $B : \mathbb{Z}_N \to \{-1, 1\}$, we have*

$$\|B \circ H\|_2 \le \mathit{bias}_B(N) + N^{o(1)} \cdot U_H(N) \ .$$

PROOF.

$$
\begin{aligned}
\|B \circ H\|_2 &\leq \mathrm{bias}_B(N) + \frac{1}{N} \sum_{d:d|N, d<N} \sum_{a \in \mathbb{Z}^*_{N/d}} |\langle B, E_{-ad}\rangle| \, \|E_{ad} \circ H\|_2 \\
&\leq \mathrm{bias}_B(N) + \frac{1}{N} \sum_{d:d|N, d<N} \max_{a \in \mathbb{Z}^*_{N/d}} \|E_{ad} \circ H\|_2 \underbrace{\sum_{a \in \mathbb{Z}^*_{N/d}} |\langle B, E_{ad}\rangle|}_{\leq N/d} \\
&\overset{(18)}{=} \mathrm{bias}_B(N) + N^{o(1)} \sum_{d:d|N, d<N} \frac{1}{d} \max_{a \in \mathbb{Z}^*_{N/d}} \|E_{ad} \circ H\|_2 \\
&\overset{(17)}{=} \mathrm{bias}_B(N) + N^{o(1)} \cdot U_H(N) \ .
\end{aligned}
$$

□

4.2 The Spectral Norm of the Auxiliary Matrices

In this section, we present a bound on the spectral norm of the complex auxiliary matrices $E_a \circ H$ for some specific functions H, namely for multiplication and exponentiation modulo N. In the former case, simple divisibility considerations and elementary arguments lead to very strong bounds on $\|E_a \circ H\|_2$. In the latter case, bounds on doubly exponential sums due to Friedlander, Konyagin, and Shparlinski [8] and Canetti et. al. [3] play a crucial role in deriving good estimates on $\|E_a \circ H\|_2$.

hier noch [3] aufgenommen

Let us start with some general considerations. For all matrices $H : \mathbb{Z}_T \times \mathbb{Z}_T \to \mathbb{Z}_N$ we have by Eq. (4):

$$
T^{1/2} \leq \|E_a \circ H\|_2 \leq T \ . \tag{19}
$$

The maximum row sum matrix norm $\|A\|_\infty$ is defined on $A \in \mathbb{C}^{T_1 \times T_2}$ as

$$
\|A\|_\infty = \max_{0 \leq x \leq T_1 - 1} \sum_{y=0}^{T_2 - 1} |A_{x,y}| \ .
$$

The following lemma is easy to show with known techniques from matrix theory (see, e.g., [13]):

Lemma 4.3 *For matrices $A \in \mathbb{C}^{T_1 \times T_2}$, $\|A\|_2^2 \leq \|AA^*\|_\infty$.*

Using (12) and (11), we see that the entries of matrix $(AA^*)_{x,y}$ with $A = E_a \circ H$ are given by

$$
(AA^*)_{x,y} = \sum_{z \in \mathbb{Z}_T} E_a(H(x,z) - H(y,z)) \ .
$$

Using Lemma 4.3, this implies the following general bound on $\|E_a \circ H\|_2$:

Lemma 4.4 *Let $H : \mathbb{Z}_T \times \mathbb{Z}_T \to \mathbb{Z}_N$ be a matrix. For all $0 \neq a \in \mathbb{Z}_N$, the following holds:*

$$\|E_a \circ H\|_2^2 \leq \|(E_a \circ H)(E_a \circ H)^*\|_\infty = \max_{x \in \mathbb{Z}_T} \sum_{y \in \mathbb{Z}_T} \left| \sum_{z \in \mathbb{Z}_T} E_a(H(x,z) - H(y,z)) \right| .$$

However, bounds on the max-expression in Lemma 4.4 are not easy to get. For this reason, we refine the lemma as follows:

Lemma 4.5 *Let $H : \mathbb{Z}_T \times \mathbb{Z}_T \to \mathbb{Z}_N$ be a matrix. For all $0 \neq a \in \mathbb{Z}_N$, the following holds:*

$$\|E_a \circ H\|_2^2 = T^{o(1)} \cdot \max_{d|T, d<T} \max_{x \in \mathbb{Z}^*_{T/d}} \sum_{y \in \mathbb{Z}^*_{T/d}} \left| \sum_{z \in \mathbb{Z}_T} E_a(H(dx,z) - H(dy,z)) \right| .$$

PROOF. We apply the "slicing-technique" from Corollary 4.2 to $\mathbb{Z}_T$ and to matrix $A := E_a \circ H$. Recall that the elements x' with $\gcd(x', T) = d$ are precisely the elements of the form $x' = xd$ where $x \in \mathbb{Z}^*_{T/d}$. Setting

$$A'_d(x,y) := \begin{cases} A(dx,y) \text{ if } x \in \mathbb{Z}^*_{T/d} \\ \quad 0 \quad\quad \text{otherwise} \end{cases} ,$$

matrix A decomposes into "slices" according to $A = \sum_{d:d|T,d<T} A'_d$. Let $A_d(x,y)$ denote the submatrix of $A'_d(x,y)$ where x ranges over $\mathbb{Z}^*_{T/d}$. Since only all-zero rows have been removed from A'_d, we conclude that $\|A_d\|_2 = \|A'_d\|_2$. Hence,

$$\|A\|_2 = \|\sum_{d:d|T,d<T} A'_d\|_2 \leq \sum_{d:d|T,d<T} \|A'_d\|_2 = \sum_{d:d|T,d<T} \|A_d\|_2 = T^{o(1)} \max_{d:d|T,d<T} \|A_d\|_2$$

where the last equation made use of (18). According to Lemma 4.3, $\|A_d\|_2 \leq \|A_d A_d^*\|_\infty$. For $x, y \in \mathbb{Z}^*_{T/d}$, the entry $(A_d A_d^*)_{x,y}$ is given by $\sum_{z \in \mathbb{Z}_T} E_a(H(dx,z) - H(dy,z))$, which concludes the proof. $\Box$

Now we are ready to bound $\|E_a \circ M\|_2$ for the function $M(x,y) = xy$ and the case $T = N$.

Lemma 4.6 *For all $0 \neq a \in \mathbb{Z}_N$, we have $\|E_a \circ M\|_2 \leq (dN)^{1/2}$, where $d = \gcd(a, N)$.*

PROOF. We write a as $d \cdot a_0$ with $\gcd(a_0, N) = 1$. For every $x, y \in \mathbb{Z}_N$,

$$\left|\sum_{z\in\mathbb{Z}_N} E_a(xz - yz)\right| = \left|\sum_{z\in\mathbb{Z}_N} E_{d\cdot a_0}(z(x-y))\right| = \left|d \sum_{z\in\mathbb{Z}_{N/d}} E_{a_0}^{N/d}(z(x-y))\right|,$$

which evaluates by Eq. (15) to N for $x = y \pmod{N/d}$ and to 0 otherwise. By Lemma 4.4, we continue with

$$\|E_a \circ M\|_2^2 \le \max_{x\in\mathbb{Z}_N} \sum_{y\in\mathbb{Z}_N} \left|\sum_{z\in\mathbb{Z}_N} E_a(xz - zy))\right| = dN \ .$$

The last equality follows since, for every fixed $x \in \mathbb{Z}_N$, $x = y \pmod{N/d}$ holds for exactly d distinct $y \in \mathbb{Z}_N$. □

According to Lemma 4.6, $\|E_{ad} \circ M\|_2 \le (dN)^{1/2}$ for all $a \in \mathbb{Z}^*_{N/d}$. With the notation from (17), we arrive at the following

Corollary 4.7

$$U_M(N) \le \max_{d:d|N, d<N} (N/d)^{1/2} \le N^{1/2} \ .$$

We move on and consider the function

$$D : \mathbb{Z}_T \times \mathbb{Z}_T \to \mathbb{Z}_N, D(x, y) = g^{xy} \ ,$$

where g is an element of order T in $\mathbb{Z}^*_N$. In order to bound $\|E_{ad} \circ D\|_2$ from above, the following results from [3,8] will be useful:

Lemma 4.8 ([8]) *Let $\gamma \in \mathbb{Z}^*_N$ be an element of order T. Let $0 \ne a \in \mathbb{Z}_N$ be an integer with $\gcd(a, N) = d < N$. Then we have the bound*

$$\sum_{x\in\mathbb{Z}_T} \left|\sum_{y\in\mathbb{Z}_T} E_a(\gamma^y - \gamma^{xy})\right| = d^{1/4} T^{21/16} N^{5/8+o(1)} \ .$$

Note that, for $d = 1$, this bound is non-trivial if $T \ge N^{10/11+\delta}$ for some positive constant δ. For prime N there is a slightly stringer bound:

Lemma 4.9 ([3]) *Let N be a prime and let $\gamma \in \mathbb{Z}^*_N$ be an element of order T. Let $0 \ne a \in \mathbb{Z}_N$ be an integer. Then we have the bound*

$$\sum_{x\in\mathbb{Z}_T} \left|\sum_{y\in\mathbb{Z}_T} E_a(\gamma^y - \gamma^{xy})\right| = T^{5/3} N^{1/4} \ .$$

Lemma 4.10 *For all $0 \neq a \in \mathbb{Z}_N$ and $d = \gcd(a, N) < N$, the following holds:*

$$\|E_a \circ D\|_2 = T^{21/32} N^{5/16+o(1)} d^{1/8} \ .$$

Furthermore, for primes N,

$$\|E_a \circ D\|_2 = T^{5/6+o(1)} N^{1/8} \ .$$

PROOF. Let us first focus on the case of composite N. According to Lemma 4.5,

$$\|E_a \circ D\|_2^2 = T^{o(1)} \cdot \max_{e|T, e<T} \max_{x \in \mathbb{Z}^*_{T/e}} \sigma_x(e) \ ,$$

where the e-slice $\sigma_x(e)$ is given by

$$\sigma_x(e) = \sum_{y \in \mathbb{Z}^*_{T/e}} \left| \sum_{z \in \mathbb{Z}_T} E_a(D(ex, z) - D(ey, z)) \right| = \sum_{y \in \mathbb{Z}^*_{T/e}} \left| \sum_{z \in \mathbb{Z}_T} E_a(g^{exz} - g^{eyz}) \right| \ . \tag{20}$$

We claim that (regardless of the choice of divisor e and $x \in \mathbb{Z}^*_{T/e}$)

$$\sigma_x(e) = T^{21/16} N^{5/8+o(1)} d^{1/4} \ ,$$

which would conclude the proof of the lemma. The claim can be seen as follows. Since g is an element of order T, the element g^e is of order T/e. Since $x \in \mathbb{Z}^*_{T/e}$, the element $\gamma := \gamma(e, x) := g^{ex}$ is of the same order. The calculation (20) is now continued to prove the claim:

$$\begin{aligned}
\sigma_x(e) \quad & \leq \quad \sum_{y \in \mathbb{Z}^*_{T/e}} \left| \sum_{z \in \mathbb{Z}_T} E_a(\gamma^z - \gamma^{yz/x}) \right| \\
& \overset{y:=y/x}{=} \quad \sum_{y \in \mathbb{Z}^*_{T/e}} \left| \sum_{z \in \mathbb{Z}_T} E_a(\gamma^z - \gamma^{yz}) \right| \\
& = \quad e \sum_{y \in \mathbb{Z}^*_{T/e}} \left| \sum_{z \in \mathbb{Z}_{T/e}} E_a(\gamma^z - \gamma^{yz}) \right| \\
& \leq \quad e \sum_{y \in \mathbb{Z}_{T/e}} \left| \sum_{z \in \mathbb{Z}_{T/e}} E_a(\gamma^z - \gamma^{yz}) \right| \\
& \overset{\text{Lemma 4.8}}{\leq} \quad e(T/e)^{21/16} N^{5/8+o(1)} d^{1/4} \\
& \overset{e \geq 1}{\leq} \quad T^{21/16} N^{5/8+o(1)} d^{1/4} \ .
\end{aligned}$$

For the case of prime N we can plug in the stronger bound from Lemma 4.9 to obtain the assertion. □

Corollary 4.11

$$U_D(N) = \max_{d:d|N, d<N} N^{5/16+o(1)} T^{21/32} d^{-7/8} = N^{5/16+o(1)} T^{21/32} \quad .$$

For primes N,

$$U_D(N) = N^{1/8} T^{5/6+o(1)} \quad .$$

4.3 Multiplicative and Exponential Structure on Subdomains

Since the spectral norm is invariant under permutations of rows and columns we have that for all bijective functions $\tilde{\sigma}, \tilde{\tau} : \{0, \ldots, T-1\} \rightarrow \mathbb{Z}_T$, and for $M_{\tilde{\sigma},\tilde{\tau}}(x, y) = M(\tilde{\sigma}(x), \tilde{\tau}(y))$,

$$\|B \circ M_{\tilde{\sigma},\tilde{\tau}}\|_2 = \|B \circ M\|_2 \quad . \tag{21}$$

In the **multiplicative case**, we may now plug-in the bound $U_M(N) \leq N^{1/2}$ (from Corollary 4.7) into Corollary 4.2 and obtain:

Corollary 4.12 *For smooth binary functions $B : \mathbb{Z}_N \rightarrow \{-1, 1\}$ and for bijective mappings $\tilde{\sigma}, \tilde{\tau} : \{0, \ldots, N-1\} \rightarrow \mathbb{Z}_N$, the following holds:*

$$\|B \circ M_{\tilde{\sigma},\tilde{\tau}}\|_2 = \|B \circ M\|_2 \leq bias_B(N) + N^{1/2+o(1)} \quad .$$

In the **exponential case**, we may similarly apply Corollary 4.2 with the upper bound $U_D(N) = T^{21/32} N^{5/16+o(1)}$ from Corollary 4.11, which leads to

Corollary 4.13 *For smooth binary functions $B : \mathbb{Z}_N \rightarrow \{-1, 1\}$ and for bijective mappings $\tilde{\sigma}, \tilde{\tau} : \{0, \ldots, T-1\} \rightarrow \mathbb{Z}_T$, the following holds:*

$$\|B \circ D_{\tilde{\sigma},\tilde{\tau}}\|_2 \leq bias_B(N) + N^{5/16+o(1)} T^{21/32} \quad .$$

A function H with a multiplicative structure coincides with $M_{\sigma,\tau}$ on a subdomain $\mathcal{X} \times \mathcal{Y}$. The "non-multiplicative behavior" outside the subdomain can however be controlled as follows:

Lemma 4.14 *If matrices $A, B : \{0, \ldots, T-1\} \times \{0, \ldots, T-1\} \rightarrow \{-1, 1\}$ coincide on subdomain $\mathcal{X} \times \mathcal{Y}$, then*

$$|\|A\|_2 - \|B\|_2| \leq 2\sqrt{T^2 - |\mathcal{X}||\mathcal{Y}|} \quad .$$

PROOF. By the triangle inequality and by (3), we obtain

$$\|A\|_2 = \|B + A - B\|_2 \leq \|B\|_2 + \|A - B\|_2 \leq \|B\|_2 + \|A - B\|_F \quad .$$

Since $A-B \in \{-2,0,2\}^{T\times T}$ is zero on subdomain $\mathcal{X}\times\mathcal{Y}$, it has at most $T^2 - |\mathcal{X}||\mathcal{Y}|$ nonzero entries of absolute value 2. Thus, $\|A-B\|_F \leq 2\sqrt{T^2 - |\mathcal{X}||\mathcal{Y}|}$, which shows one direction of the lemma. For reasons of symmetry, the other direction holds as well. □

Now we are ready to prove Theorem 3.4:

PROOF. [of Theorem 3.4] Let B be a balanced binary function. Let H be a function with multiplicative structure on subdomain $\mathcal{X}\times\mathcal{Y}$ of $\{0,\ldots,N-1\}\times\{0,\ldots,N-1\}$. By Definition 3.1 there exist injective functions $\sigma:\mathcal{X}\to\mathbb{Z}_N$ and $\tau:\mathcal{Y}\to\mathbb{Z}_N$, such that H coincides with $M_{\sigma,\tau}$ on subdomain $\mathcal{X}\times\mathcal{Y}$. Since the mapping $\sigma:\mathcal{X}\to\mathbb{Z}_N$ is injective, it can be extended to a bijective mapping from $\{0,\ldots,N-1\}$ to $\mathbb{Z}_N$ without changing its behavior on $\mathcal{X}$. The same remark holds for τ. Let $\tilde{\sigma},\tilde{\tau}:\{0,\ldots,N-1\}\to\mathbb{Z}_N$ be the resulting bijective functions. Then $B\circ M_{\sigma,\tau}$ coincides with $B\circ M_{\tilde{\sigma},\tilde{\tau}}$ on subdomain $\mathcal{X}\times\mathcal{Y}$. The part outside of the subdomain can be controlled by Lemma 4.14:

$$\|B\circ H\|_2 \leq \|B\circ M_{\tilde{\sigma},\tilde{\tau}}\|_2 + 2\sqrt{N^2 - |\mathcal{X}||\mathcal{Y}|}\ .$$

Making use of Corollary 4.12 and of the assumption that B is balanced, we get

$$\begin{aligned}\|B\circ M_{\tilde{\sigma},\tilde{\tau}}\|_2 &\leq \mathrm{bias}_B(N) + N^{1/2+o(1)} + 2\sqrt{N^2 - |\mathcal{X}||\mathcal{Y}|}\\ &= N^{1/2+o(1)} + 2\sqrt{N^2 - |\mathcal{X}||\mathcal{Y}|}\ .\end{aligned}$$

Since

$$\begin{aligned}N^2 - |\mathcal{X}||\mathcal{Y}| &= N(N-|\mathcal{X}|) + N(N-|\mathcal{Y}|) - (N-|\mathcal{X}|)(N-|\mathcal{Y}|)\\ &\leq N(N-|\mathcal{X}|) + N(N-|\mathcal{Y}|)\end{aligned}$$

and (by assumption) $N-|\mathcal{X}| = O(N^\alpha)$ and $N-|\mathcal{Y}| = O(N^\alpha)$ for some fixed constant $0\leq\alpha<1$, we finally arrive at

$$\|B\circ H\|_2 = N^{1/2+o(1)} + O(N^{(1+\alpha)/2})\ ,$$

which concludes the proof. □

Theorem 3.5 follows analogously by combining Corollary 4.13 with Lemma 4.14. In the special case of prime N, we may use the stronger bound from Corollary 4.11 to obtain the bound of Theorem 3.6.

5 Applications

In Section 3.3 we proved that balanced Boolean predicates of functions with multiplicative or exponential structure have relatively small spectral norms. Now we present some natural functions having multiplicative or exponential structure (on a large subdomain).

5.1 Discrete Multiplication and Division modulo arbitrary Integers

Applying Theorem 3.4 (with $\mathcal{X} = \mathcal{Y} = \{0, \ldots, N-1\}$ and $\sigma, \tau : \{0, \ldots, N-1\} \to \mathbb{Z}_N$ defined as the identity) to the function M, we immediately get:

Corollary 5.1 *For balanced Boolean functions $B : \mathbb{Z}_N \to \{-1, 1\}$,*

$$\|B \circ M\|_2 = N^{1/2+o(1)} \ .$$

We say a function $D : \{0, \ldots, N-1\} \times \{0, \ldots, N-1\} \to \mathbb{Z}_N$ *performs discrete division*, if it satisfies

$$\gcd(y, N) = 1 \implies D(x, y) = x/y \ .$$

(We don't care about the function values when $\gcd(y, N) \neq 1$.) In the sequel, notation DIV is reserved for functions performing discrete division. Since discrete division is nothing but one inversion (permutation) plus discrete multiplication, we get the following

Corollary 5.2 *For integers N with $N - \varphi(N) = O(N^\alpha)$ for some fixed constant $\alpha > 0$,*[4] *and for balanced Boolean functions $B : \mathbb{Z}_N \to \{-1, 1\}$, the following holds:*

$$\|B \circ DIV\|_2 = O(N^{(1+\alpha)/2}) \ .$$

If N is prime, this can be strengthened to

$$\|B \circ DIV\|_2 = N^{1/2+o(1)} \ .$$

PROOF. Let $\mathcal{X} = \{0, \ldots, N-1\}$ and $\mathcal{Y} = \{0, \ldots, N-1\}^*$. Define the injective mapping $\tau : \mathcal{Y} \to \mathbb{Z}_N$ as $\tau(y) := y^{-1} \bmod N$. With $\sigma : \mathcal{X} \to \mathbb{Z}_N$ given by the identity, we have

$$DIV(x, y) = xy^{-1} = x\tau(y) = M_{\sigma,\tau}(x, y)$$

[4] This is the case, for example, for integers N whose smallest prime-factor is of the order $\Omega(N^{1-\alpha})$.

for all $(x, y) \in \mathcal{X} \times \mathcal{Y}$ showing that DIV has multiplicative structure on subdomain $\mathcal{X}\times\mathcal{Y}$. Noting that $N-|\mathcal{X}| = 0$ and $N-|\mathcal{Y}| = N-\varphi(N) = O(N^\alpha)$, the result follows from Theorem 3.4. □

5.2 Discrete Exponentiation modulo Primes

For primes N, the discrete power function $POW : \{0, \ldots, N-1\} \times \{0, \ldots, N-2\} \to \mathbb{Z}_N^*$ is given by

$$POW(x, y) = x^y \bmod N \ .$$

Corollary 5.3 *For primes N and for balanced binary functions $B : \mathbb{Z}_N \to \{-1, 1\}$, we have*

$$\|B \circ POW\|_2 = N^{23/24+o(1)} \ .$$

PROOF. Let $\mathcal{X} := \{1, \ldots, N-1\}$ and $\mathcal{Y} := \{0, \ldots, N-2\}$. Because of Theorem 3.6, it suffices to show that POW has exponential structure on subdomain $\mathcal{X} \times \mathcal{Y}$ w.r.t. a primitive root g in $\mathbb{Z}_N^*$ (of order $N-1$). To this end, let $\sigma : \mathcal{X} \to \mathbb{Z}_{N-1}$ and $\tau : \mathcal{Y} \to \mathbb{Z}_{N-1}$ be injective functions given by $x = g^{\sigma(x)}$ and $\tau(y) = y$, respectively. In other words, σ is chosen as the discrete logarithm and τ is the identity function. Now, the exponential structure becomes obvious because

$$POW(x, y) = x^y = g^{\sigma(x)\tau(y)} = D_{\sigma,\tau}(x, y)$$

holds for all $x \in \mathcal{X}$ and $y \in \mathcal{Y}$. □

5.3 Cryptographic Applications

As we saw in the last section our two main theorems can be applied to some basic functions with multiplicative and exponential structure. In this section we show that our techniques can also be applied to functions appearing naturally in cryptographic protocols. To simplify notation we will sometimes, when it is clear to the reader, identify the set $\mathbb{Z}_N$ with the set of integers $\{0, \ldots, N-1\}$ and vice versa.

Example 5.4 (Pointcheval Cryptosystem [22]) *Let N be an RSA modulus, i.e., $N = pq$ for two primes p, q of (roughly) the same bit length. Let e be an integer with $\gcd(e, \varphi(N)) = 1$. The tuple (N, e) is the public key and an integer d with $ed = 1 \bmod \varphi(N)$ is the secret key. Note that by the knowledge of either p or q, $\varphi(N) = (p-1)(q-1)$ can be computed and so can d. The* *following function*

$$F : \mathcal{R} \times \mathbb{Z}_N \to \mathbb{Z}_N^* \times \mathbb{Z}_N, \quad F(r,m) = ((r-1)^e, r^e \cdot m),$$

where $r \in \mathcal{R} = \{r \in \mathbb{Z}_N : r-1 \in \mathbb{Z}_N^*\}$ *is chosen at random, encrypts a message* m*. Note that it can be evaluated by knowledge of the public key* (N,e) *only. Define* $\mathcal{X} := \{x : x^d + 1 \in \mathbb{Z}_N^*\}$ *and note that* $|\mathcal{X}| = \varphi(N)$*. As for decryption (given the "secret key"* d*), we may use any function* $H : \{0,\ldots,N-1\} \times \{0,\ldots,N-1\} \to \mathbb{Z}_N$ *that satisfies* $H(x,y) = y(x^d+1)^{-e}$ *for all* $x \in \mathcal{X}$ *and* $y \in \mathcal{Y} = \{0,\ldots,N-1\}$*. It is easy to check that this implies that* $H((r-1)^e, r^e \cdot m) = m$ *for all* $r \in \mathcal{R}$*. Outside the subdomain* $\mathcal{X} \times \mathcal{Y}$ *(when* H *is applied to invalid ciphers), we may however allow* H *to attain arbitrary values. The mapping* $\sigma : \mathcal{X} \to \mathbb{Z}_N^*$ *given by* $\sigma(x) := (x^d+1)^{-e}$ *defines a bijection. With* $\tau : \mathcal{Y} \to \mathbb{Z}_N$ *defined as the identity, we have*

$$H(x,y) = \sigma(x)y = M_{\sigma,\tau}(x,y)$$

for all $x \in \mathcal{X}$ *and* $y \in \mathcal{Y}$*, and we may conclude that any correct decryption function* H *has a multiplicative structure on subdomain* $\mathcal{X} \times \mathcal{Y}$*. Since* $|\mathcal{X}| = \varphi(N) = (p-1)(q-1)$*, the part outside the subdomain has a relatively small size:* $N - |\mathcal{X}| = N - \varphi(N) = p + q - 1 \approx 2N^{1/2}$*.*

Example 5.5 (El Gamal Cryptosystem [9]) *Let* N *be a prime modulus and let* $g \in \mathbb{Z}_N^*$ *be an element of order* $N-1$*. The "public key" has the form* $h = g^s$ *for some* $s \in \mathbb{Z}_{N-1}$*. A message* $m \in \mathbb{Z}_N$ *is encrypted with "randomness"* $r \in \mathbb{Z}_{N-1}$ *by evaluating the function*

$$F : \mathbb{Z}_{N-1} \times \mathbb{Z}_N \to \mathbb{Z}_N^* \times \mathbb{Z}_N, \quad F(r,m) = (g^r, h^r m).$$

As for decryption (given the "secret key" s*), we may use any function* $H : \{0,\ldots,N-1\} \times \{0,\ldots,N-1\} \to \mathbb{Z}_N$ *that satisfies* $H(x,y) = yx^{-s}$ *for all* $x \in \mathcal{X} := \{1,\ldots,N-1\}$ *and all* $y \in \mathcal{Y} := \{0,\ldots,N-1\}$*. It is easy to check that* $H(g^r, h^r m) = m$*. Since for the injective mappings* $\sigma : \mathcal{X} \to \mathbb{Z}_N$ *given by* $\sigma(x) := x^{-s}$*, and* $\tau : \mathcal{Y} \to \mathbb{Z}_N$ *given by the identity,* H *satisfies*

$$H(x,y) = yx^{-s} = y\sigma(x) = M_{\sigma,\tau}(x,y),$$

for all $x \in \mathcal{X}$ *and* $y \in \mathcal{Y}$*, we may conclude that* H *has a multiplicative structure on subdomain* $\mathcal{X} \times \mathcal{Y}$*. Note that* $N - |\mathcal{X}| = N - (N-1) = 1$*.*

In all these examples we have a multiplicative structure (Definition 3.1) on different (but sufficiently large) subdomains. Combining it with Theorem 3.4 we get the following:

Corollary 5.6 *Let* B *be a balanced binary function.*

(1) Let $H : \{0,\ldots,N-1\} \times \{0,\ldots,N-1\} \to \mathbb{Z}_N$ *be a decryption function of the Pointcheval cryptosystem. Then,* $\|B \circ H\|_2 = O(N^{3/4})$*.*

(2) Let $H : \{0, \ldots, N-1\} \times \{0, \ldots, N-1\} \to \mathbb{Z}_N$ be a decryption function of the El Gamal cryptosystem Then, $\|B \circ H\|_2 = N^{1/2+o(1)}$.

In general, for all cryptosystems that follow the El Gamal structure we can show such upper bounds on the spectral norm of the decryption functions. For more examples the reader is referred to the RSA-Paillier cryptosystem [4] (which is a modification of the original cryptosystem of Paillier [20]).

For an element g of order T in $\mathbb{Z}_N^*$, let $G \subseteq \mathbb{Z}_N^*$ be the subgroup generated by g. For an element $x \in G$ we denote by $\log_g x$ the discrete logarithm of x to the basis g, i.e. the (unique) element $a \in \mathbb{Z}_T$ that satisfies $g^a = x$. If T contains at least one large prime factor, then computing the discrete logarithm in G is assumed to be computationally hard. The *Diffie-Hellman function* [5] $DH : G \times G \to G$ with respect to g is given by the following mapping:

$$DH(x, y) = g^{\log_g x \cdot \log_g y} \ .$$

The security of numerous cryptographic protocols relies on the computational hardness of computing this function. The most famous of those protocols is the Diffie-Hellman key exchange protocol (see [5] or, e. g. [19, Chapters 3.7 and 12.6]) itself: Alice and Bob respectively pick random $a, b \in \mathbb{Z}_T$ and exchange $x = g^a, y = g^b$. The secret key, $g^{ab} = g^{\log_g x \cdot \log_g y}$, can be computed by both parties. In order to totally break the protocol, a passive eavesdropper, Eve, must compute the Diffie-Hellman function. Again, if T contains at least one large prime factor, then computing the Diffie-Hellman function in G is assumed to be computationally hard (*computational Diffie-Hellman assumption*). As an example of a cryptosystem whose security relies on the Diffie-Hellman function we can mention the El Gamal Cryptosystem [9] (see also Example 5.5).

We proceed with two examples for functions H with exponential structure.

Corollary 5.7 (Diffie-Hellman secret modulo primes) *For primes N, for elements g of order $T = N - 1$, and for balanced binary functions $B : \mathbb{Z}_N \to \{-1, 1\}$, we have $\|B \circ DH\|_2 = N^{23/24+o(1)}$.*

PROOF. The proof is similar to the proof of Corollary 5.3. Let $\mathcal{X} := \mathcal{Y} := \{1, \ldots, N-1\}$. Because of Theorem 3.6, it suffices to show that DH has exponential structure on subdomain $\mathcal{X} \times \mathcal{Y}$ w.r.t. a primitive root g in $\mathbb{Z}_N^*$ (of order $N-1$). To this end, let $\sigma : \mathcal{X} \to \mathbb{Z}_{N-1}$ be the injective function given by $x = g^{\sigma(x)}$ (the discrete logarithm). Now, the exponential structure becomes obvious because

$$DH(x, y) = g^{\sigma(x)\sigma(y)} = D_{\sigma,\sigma}(x, y)$$

holds for all $x \in \mathcal{X}$ and $y \in \mathcal{Y}$. □

The next example can be viewed as "computing the Diffie-Hellman function given the secret keys." Let N be an arbitrary modulus and let g be an element of order T. To compute the Diffie-Hellman secret given x and y, we may use the function $D : \{0, \ldots, T-1\} \times \{0, \ldots, T-1\} \to \mathbb{Z}_N$ given by

$$D(x, y) = g^{xy}.$$

The following corollary follows directly from Theorem 3.5 and Theorem 3.6 (applied with $\mathcal{X} = \mathcal{Y} = \{0, \ldots, N-2\}$ and $\tau, \sigma : \{0, \ldots, N-2\} \to \mathbb{Z}_{N-1}$ defined as the identity):

Corollary 5.8 (Discrete exponentiation modulo arbitrary integers) *For elements g of order $T = N-1$, and for balanced binary functions $B : \mathbb{Z}_N \to \{-1, 1\}$, we have*

$$\|B \circ D\|_2 = N^{31/32+o(1)} \quad .$$

For primes N, the functions DH and D used in Corollaries 5.7 and 5.8 only differ by a permutation of rows and columns such that their spectral norms are equal. This is despite the fact that, in the unrestricted model of computation, D is easy to compute whereas DH is believed to be not. Thus there is no hope to prove superpolynomial lower bounds in an unrestricted model of computation that are solely based on the spectral norm of the function.

6 Final Remarks

In this final section, we illustrate three things. First, the family of matrices that represent "bits" of discrete multiplication is fairly rich: for any value in the range between $N^{1/2}$ and N, we actually find a matrix from this family whose spectral norm (roughly) coincides with this value. Second, the upper bounds on the spectral norm given by Corollaries 4.12 and 4.13 are asymptotically tight when the bias-term becomes asymptotically dominant. Third, the main result from Theorem 3.4 can be easily generalized to the case of arbitrary bivariate polynomials.

6.1 Matrices with Small Spectral Norm

The spectral norm of a matrix $H \in \{-1, 1\}^{N \times N}$ attains its smallest possible value $N^{1/2}$ iff the matrix has orthogonal rows (or columns), i.e., iff $HH^\top = NI_N$. A matrix with this property is called a generalized Hadamard matrix. It can only exist if $N \in \{1, 2\}$ or if N is divisible by 4 [1,11]. This raises the question whether, say for odd values of N, there are other natural families of matrices from $\{-1, 1\}^{N \times N}$ whose spectral norm comes close to the (unreachable) barrier $N^{1/2}$. As a by-product of Theorem 3.4, this question can be answered in the positive: for any balanced binary function B and for any function H with a multiplicative structure on a large subdomain of $\mathbb{Z}_N \times \mathbb{Z}_N$ (such that parameter α in Theorem 3.4 can be set to 0), we have $\|B \circ H\|_2 = N^{1/2+o(1)}$. In particular, this holds for B_0 (the least significant bit) and M (discrete multiplication). For B_0 and M, the function hidden in the term $N^{o(1)}$ can sometimes be determined more precisely. Consider the case of odd N. Lemma A.5 shows that $EXP_{B_0}(N, 1) \leq 3 \log N$. From the Splitting Lemma (Lemma 4.1), we may infer that

$$\|B_0 \circ M\|_2 \leq 1 + 3N^{1/2} \log N \ .$$

6.2 The "Bias-Barrier" and Matrices of Arbitrary Spectral Norm

We claim that the bounds from Corollaries 4.12 and 4.13 cannot be improved beyond the value $\mathrm{bias}_B(N)$. In order to show this claim, we start with the following result:

Lemma 6.1 *If every column (or row, respectively) of a matrix $H : \mathbb{Z}_N \times \mathbb{Z}_N \to \mathbb{Z}_N$ represents a permutation of $\mathbb{Z}_N$, then $\|B \circ H\|_2 \geq \mathit{bias}_B(N)$.*

PROOF. Say the columns of matrix H represent permutations of $\mathbb{Z}_N$. Then, for any $y \in \mathbb{Z}_N$, we have $\sum_{x \in \mathbb{Z}_N} B(H(x, y)) = \mathrm{bias}_B(N)$ and therefore

$$1/N \sum_{x,y \in \mathbb{Z}_N} B(H(x, y)) = \mathrm{bias}_B(N) \ .$$

Now we can lower bound the spectral norm of $B \circ H$ in the following way:

$$\|B \circ H\|_2 \geq \left| \sum_{x,y \in \mathbb{Z}_N} \frac{1}{\sqrt{N}} B(H(x, y)) \frac{1}{\sqrt{N}} \right| = \mathrm{bias}_B(N) \ . \tag{22}$$

□

By changing $N^2 - \varphi^2(N)$ entries, the matrix M with $M(x, y) = xy$ can be transformed into a matrix M' whose rows and columns represent permutations of $\mathbb{Z}_N$. Lemma 4.14 (applied with $|\mathcal{X}| = |\mathcal{Y}| = \varphi(N)$) leads to $|\|B \circ M\|_2 - \|B \circ M'\|_2| \leq 2\sqrt{N^2 - \varphi^2(N)}$ and thus, by Lemma 6.1, we get

$$\|B \circ M\|_2 \geq \mathrm{bias}_B(N) - 2\sqrt{N^2 - \varphi^2(N)} \ . \tag{23}$$

We would like to make $\text{bias}_B(N)$ the asymptotically dominant term. Note first that $\sqrt{N^2 - \varphi^2(N)} = \sqrt{2N-1}$ if N is prime. In order to get a smooth binary function whose bias asymptotically grows faster than $\sqrt{N}$, we proceed as follows. Let $I \subseteq \mathbb{Z}_N$ be any consecutive interval of length $(N - N^{1/2+\varepsilon})/2$ for a constant $0 < \varepsilon < 1/2$. Define $B_\varepsilon : \mathbb{Z}_N \to \{-1, 1\}$ as the Boolean function that evaluates to 1 if and only if its input x belongs to the interval I. Obviously we have $\text{bias}_{B_\varepsilon}(N) = N^{1/2+\varepsilon}$. Thus,

$$\|B_\varepsilon \circ M\|_2 \geq (1 + o(1))\text{bias}_B(B_\varepsilon) \ .$$

Using tools that are explained in the appendix, it is easy to show that B_ε is smooth.[5] Thus, Corollary 4.12 yields the upper bound

$$\|B_\varepsilon \circ M\|_2 \leq (1 + o(1))N^{1/2+\varepsilon} \ .$$

We see that upper and lower bound match each other asymptotically.

As a by-product of our discussion, we see that the family of matrices that represent "bits" of discrete multiplication is rich enough to contain matrices of (roughly) any spectral norm of our choice.

6.3 Extensions

For the case of prime N the main result of Theorem 3.4 can be generalized to the case of arbitrary bivariate polynomials of bounded degree using the well known Weil bound for exponential sums [28] (see also [17]):

Lemma 6.2 *For primes N, $a \in \mathbb{Z}_N^*$, and any a_i with $\gcd(a_0, a_1, \ldots, a_k, N) = 1$, we have*

$$\left| \sum_{x \in \mathbb{Z}_N} E_a(a_0 + a_1 x + \ldots + a_k x^k) \right| \leq (k-1)N^{1/2} \ .$$

Corollary 6.3 *For primes N let $P : \mathbb{Z}_N \times \mathbb{Z}_N \to \mathbb{Z}_N$ be a bivariate polynomial of maximal degree $O(N^\alpha)$ for a constant $0 \leq \alpha < 1/2$. Then, for balanced binary functions B,*

$$\|B \circ P\|_2 = N^{3/4+\alpha/2+o(1)} \ .$$

PROOF. Write P as $P(x,y) = \sum_{i=0}^{k} \sum_{j=0}^{k} a_{ij} x^i y^j$, where $k = O(N^\alpha)$. For every fixed $x, y \in \mathbb{Z}_N$, $Q(x,y,z) := P(x,z) - P(y,z)$ is a polynomial of degree

[5] It turns out that B_ε is strongly semilinear of length 1 in the sense of Definition A.1. Then, smoothness follows from Lemma A.2.

at most k in the indeterminate z:

$$Q(x,y,z) = \sum_{j=0}^{k} a_j(x,y)z^j, \quad a_j(x,y) = \sum_{i=0}^{k} a_{ij}(x^i - y^i) \ .$$

For fixed $x \in \mathbb{Z}_N$, there can be at most k different $y \in \mathbb{Z}_N$ such that $Q(x,y,z)$ equals the zero polynomial in the indeterminate z. We denote those y by the exceptional set E_x ($|E_x| \leq k$ for all $x \in \mathbb{Z}_N$). For every other $y \notin E_x$ we have $\gcd(a_1(x,y), a_2(x,y), \ldots, a_k(x,y), N) = 1$ (since there must be at least one coefficient $a_j(x,y) \neq 0$) and, by Lemma 6.2,

$$\left| \sum_{z \in \mathbb{Z}_N} E_a(P(x,z) - P(y,z)) \right| = \left| \sum_{z \in \mathbb{Z}_N} E_a(Q(x,y,z)) \right|$$

can be bounded by $(k-1)N^{1/2}$ for $y \notin E_x$ and by N for $y \in E_x$. By Lemma 4.4 we continue with

$$\begin{aligned} \|E_a \circ P\|_2^2 &\leq \max_{x \in \mathbb{Z}_N} \sum_{y \in \mathbb{Z}_N} \left| \sum_{z \in \mathbb{Z}_N} E_a(P(x,z) - P(z,y)) \right| \\ &\leq (N-k)(k-1)N^{1/2} + kN \\ &= O(kN^{3/2}) \ . \end{aligned}$$

Then the assertion follows by Corollary 4.2 (with $d = 1$). □

References

[1] J. Brenner and L. Cummings. The Hadamard maximum determinant problem. *Amer. Math. Monthly*, 79:626–630, 1972.

[2] J. Bruck. Harmonic analysis of polynomial threshold functions. *SIAM Journal on Discrete Mathematics*, 3(2):168–177, May 1990.

[3] R. Canetti, J. B. Friedlander, S. V. Konyagin, M. Larsen, D. Lieman, and I. E. Shparlinski. On the statistical properties of Diffie-Hellman distributions. *Israel J. Math.*, 120:23–46, 2000.

[4] D. Catalano, R. Gennaro, N. Howgrave-Graham, and P. Q. Nguyen. Paillier's cryptosystem revisited. In *Proceedings of the 8th ACM Conference on Computer and Communications Security*, pages 206–214, 2001.

[5] W. Diffie and M. Hellman. New directions in cryptography. *IEEE Transactions on information Theory*, 22(6):644–654, 1976.

[6] J. Forster. A linear lower bound on the unbounded error probabilistic communication complexity. *Journal of Computer and System Sciences*, 65(4):612–625, 2002.

[7] J. Forster, M. Krause, S. V. Lokam, R. Mubarakzjanov, N. Schmitt, and H. U. Simon. Relations between communication complexity, linear arrangements, and computational complexity. In *Proceedings of the Conference on Foundations of Software Technology and Theoretical Computer Science*, pages 171–182, 2001.

[8] J. B. Friedlander, S. V. Konyagin, and I. E. Shparlinski. Some doubly exponential sums over $\mathbb{Z}_m$. *Acta Arithm.*, 105:349–370, 2002.

[9] T. El Gamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *Advances in Cryptology—CRYPTO '84*, pages 10–18, 1984.

[10] M. Goldmann, J. Håstad, and A. A. Razborov. Majority gates versus general weighted threshold gates. *Journal of Computational complexity*, 2:277–300, 1992.

[11] J. Hadamard. Résolution d'une question relative aux déterminants. *Bull. Sci. Math.*, 17:240–246, 1893.

[12] A. Hajnal, W. Maass, P. Pudlak, M. Szegedy, and G. Turan. Threshold circuits of bounded depth. *Journal of Computer and System Sciences*, 46:129–154, 1993.

[13] R. A. Horn and C. R. Johnson. *Matrix analysis*. Cambridge Univ. Press, 1991.

[14] E. Kiltz. On the representation of boolean predicates of the Diffie-Hellman function. In *Proc. of 20th International Symposium on Theoretical Aspects of Computer Science STACS*, pages 223–233, 2003.

[15] E. Kiltz. *Complexity Theoretic Lower Bounds on Cryptographic Functions*. PhD thesis, Ruhr-Universität Bochum. Availabe from: http://www-brs.ub.ruhr-uni-bochum.de/netahtml/HSS/Diss/KiltzEike/, 2004.

[16] E. Kiltz and H. U. Simon. Complexity theoretic aspects of some cryptographic functions. *Proceedings of the Ninth International Computing and Combinatorics Conference, COCOON 2003, LNCS 2697*, pages 294–303, 2003.

[17] N. M. Korobov. *Exponential Sums and their Applications*. Kluwer Academic Publishers, 1992.

[18] M. Krause and I. Wegener. Circuit complexity. *Boolean Functions Vol. II*, to appear.

[19] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone. *Handbook of applied cryptography*. CRC Press, Boca Raton, 1997.

[20] P. Paillier. Public-key cryptosystems based on composite degree residuosity classes. *Advances in Cryptology – Proceedings of EUROCRYPT '99*, pages 223–238, 1999.

[21] R. Paturi and J. Simon. Probabilistic communication complexity. *Journal of Computer and System Sciences*, 33(1):106–123, 1986.

[22] D. Pointcheval. New public key cryptosystems based on the dependent — RSA problems. In *Advances in Cryptology - Proceedings of EUROCRYPT '99*, pages 239–254. LNCS, Springer-Verlag, 1999.

[23] K. Prachar. *Primzahlverteilung.* Springer-Verlag, Berlin, 1957.

[24] R. Shaltiel. Towards proving strong direct product theorems. In *Proceedings of the Sithteenth Annual Conference on Computational Complexity*, pages 107–119. IEEE Computer Society, 2001.

[25] I. E. Shparlinski. Communication complexity and Fourier coefficients of the Diffie-Hellman key. *Proc. the 4th Latin American Theoretical Informatics Conf., LNCS 1776*, pages 259–268, 2000.

[26] I. E. Shparlinski. *Cryptographic Application of Analytic Number Theory: Complexity Lower Bounds and Pseudorandomness*, Volume 22 of *Progress in Computer Science and Applied Logic.* Birkhäuser Verlag, 2003.

[27] I. M. Vinogradov. *Elements of number theory.* Dover Publications, 1954.

[28] A. Weil. On some exponential bounds. *Proc. Nat. Acad. Sci. USA*, 35(5):204–207, 1948.

A Upper Bounds on the Balance Terms

For every integer $N > 6$ let $M(a)$ and $P(a)$ be functions such that $P(a) \geq 0$ for $a \in \{1, \ldots, N-1\}$. As an easy consequence (see [27], Chapter 3, Ex. 11c) of (14), one gets

$$\frac{1}{N}\sum_{a=1}^{N-1}\left|\sum_{x=M(a)}^{M(a)+P(a)} E_a(x)\right| \leq c \log N \ , \tag{A.1}$$

where $\log N = \log_2 N$ denotes the binary logarithm of N and the constant c is given by $c = \ln 2 \approx 0.6931$. As another easy consequence, we get

$$\max_{a\in\mathbb{Z}_N\setminus\{0\}}\left|\frac{E_a(P)-1}{E_a(1)-1}\right| = \left|\sum_{z=0}^{P-1} E_a(z)\right| \leq \min\{P, N-P\} \ . \tag{A.2}$$

$z =$ 0 bis $P-1$ statt $z =$ 1 bis P wegen (14)

Recall the definitions of the terms $\text{bias}_B(N)$ and $EXP_B(N,d)$ from Section 3.2. In this section we will provide bounds on the balance terms $\text{bias}_B(N)$ and $EXP_B(N,d)$ for some Boolean functions B thereby proving Theorem 3.7. We start by introducing some notation. Let $B : \mathbb{Z}_N \to \{-1, 1\}$ be a binary function. The set of integers $x \in \mathbb{Z}_N$ where B evaluates to $+1$ is denoted as B^+:

$$B^+ = \{x \in \mathbb{Z}_N : B(x) = 1\}.$$

Similarly, we define the set $B^- := \mathbb{Z}_N \setminus B^+ = \{x \in \mathbb{Z}_N : B(x) = -1\}$ as the set of integers where B evaluates to -1.

Definition A.1 *Function* $B : \mathbb{Z}_N \to \{-1, 1\}$ *is called* semilinear of length k *if there exist parameters* $M_i, L_i \in \mathbb{Z}_N$ *and* $K_i \in \mathbb{Z}_N^*$ *such that, for all* $z \in \mathbb{Z}_N$*, condition*

$$B^+ = \bigcup_{i=1\ldots k} J_i, \quad J_i := \{K_i z + M_i \bmod N |\ 0 \le z \le L_i\},$$

is valid and the sets J_i *are pairwise disjoint. We call a function* B strongly semilinear of length k *if* B *and* $-B$ *both are semilinear of length* k*.*

There are many natural strongly semilinear functions, for instance each indicator function of a union of k disjoint intervals in $\mathbb{Z}_N$ is strongly semilinear of length k.

Lemma A.2 *Let* $B : \mathbb{Z}_N \to \{-1, 1\}$ *be strongly semilinear of length* k*. Then, for every divisor* $d < N$ *of* N*,* $EXP_B(N, d) \le 2k \log(N/d)$*.*

PROOF. Let C_+ be the function obtained from B by setting $C_+(z) = 1$ if $B(z) = 1$ and $C_+(z) = 0$ if $B(z) = -1$. Let C_- be the function obtained from B by setting $C_-(z) = 1$ if $B(z) = -1$ and $C_-(z) = 0$ if $B(z) = 1$. Use $B = C_+ - C_-$ and the triangle inequality to obtain

$$EXP_B(N, d) \le \frac{d}{N} \cdot \sum_{a \in \mathbb{Z}^*_{N/d}} |\langle C_+, E_{ad} \rangle| + \frac{d}{N} \cdot \sum_{a \in \mathbb{Z}^*_{N/d}} |\langle C_-, E_{ad} \rangle| \quad . \tag{A.3}$$

Since B is strongly semilinear of length k, we characterize the function C_+ as

$$C_+(z) = 1 \Leftrightarrow z \in B^+ = \bigcup_{i=1\ldots k} J_i, \quad J_i = \{K_i z + M_i \bmod N |\ 0 \le z \le L_i\},$$

for some integer values K_i, M_i, and L_i. Using the fact that $E_{ad}(x) = E_a^{N/d}(x)$, we bound the first sum by

$$\begin{aligned}
\sum_{a \in \mathbb{Z}^*_{N/d}} \left| \langle B^+, E_{ad} \rangle \right| &= \sum_{a \in \mathbb{Z}^*_{N/d}} \left| \sum_{i=1}^{k} \sum_{z=0}^{L_i} E_a^{N/d}(K_i z + M_i) \right| \\
&\overset{(11)}{=} \sum_{a \in \mathbb{Z}^*_{N/d}} \left| \sum_{i=1}^{k} \sum_{z=0}^{L_i} E_a^{N/d}(M_i) E_a^{N/d}(K_i z) \right| \\
&\le \sum_{a \in \mathbb{Z}^*_{N/d}} \sum_{i=1}^{k} \left| E_a^{N/d}(M_i) \right| \left| \sum_{z=0}^{L_i} E_a^{N/d}(K_i z) \right| \\
&\overset{(10)}{=} \sum_{i=1}^{k} \sum_{a \in \mathbb{Z}^*_{N/d}} \left| \sum_{z=0}^{L_i} E_a^{N/d}(K_i z) \right| .
\end{aligned}$$

Since $K_i \in \mathbb{Z}_{N/d}^*$ (because $K_i \in \mathbb{Z}_N^*$), we can substitute a/K_i for a for every $1 \leq i \leq k$. After rearranging the sum we obtain by (A.1)

$$\sum_{i=1}^{k} \sum_{a \in \mathbb{Z}_{N/d}^*} \left| \sum_{z=0}^{L_i} E_a^{N/d}(z) \right| \leq \sum_{i=1}^{k} \sum_{a=1}^{N/d-1} \left| \sum_{z=0}^{L_i} E_a^{N/d}(z) \right| \leq k \frac{N}{d} \log(N/d).$$

Since the second sum in (A.3) can be bounded analogously the proof is complete. □

Now we will give a bound on the balance terms of the kth least significant bit B_k of (the binary representation of) $x \in \mathbb{Z}_N$.

We will now give a full description of the function B_k in terms of the sets B_k^+ and B_k^-. We start with the case of the *least significant bit* B_0. For the predicate $B(x) = B_0(x)$ it obviously holds that $B_0(x) = 1$ iff $x = 2z + 1$ for $0 \leq z \leq \lfloor N/2 \rfloor$. Thus, the set B_0^+ can be described by

$$B_0^+ = \{2z + 1\}_{0 \leq z \leq \lfloor N/2 \rfloor}.$$

For the inner bits B_k this characterization is getting a little bit more sophisticated. Put $r_k = N \bmod 2^{k+1}$.

$$B_k^- = \{2^{k+1} z + t\}_{0 \leq t \leq 2^k - 1, 0 \leq z \leq b_{r_k}(t)}, \tag{A.4}$$

where $b_{r_k}(t) \in \{T-1, T\}$ and T is defined as $T = \lfloor N/2^{k+1} \rfloor$. To avoid a wrap modulo N we have to choose $b_{r_k}(t) \in \{T-1, T\}$ such that the inequality

$$N - 1 - 2^{k+1} < b_{r_k}(t) 2^{k+1} + t \leq N - 1$$

holds. By $T 2^{k+1} = N - r_k$ we get

$$b_{r_k}(t) = \begin{cases} T - 1 & : \quad t \geq r_k \\ T & : \quad \text{else.} \end{cases} \tag{A.5}$$

With similar arguments as above we get:

$$\begin{aligned} B_k^+ &= \{2^{k+1} z + t\}_{2^k \leq t \leq 2^{k+1} - 1, 0 \leq z \leq b_{r_k}(t)} \\ &= \{2^{k+1} z + t + 2^k\}_{0 \leq t \leq 2^k - 1, 0 \leq z \leq b_{r_k}(t)} \end{aligned} \tag{A.6}$$

Obviously, if the modulus N is not a power of 2, the kth bit B_k is not unbiased in general. This is made precise in the following lemma:

Lemma A.3 $\mathit{bias}_{B_k}(N) = \min\{N \bmod 2^{k+1}, 2^{k+1} - N \bmod 2^{k+1}\}$.

PROOF. If 2^{k+1} divides N, the bias is zero and the result holds true. If not, we cut the elements of $\mathbb{Z}_N$ into $t := \lfloor N/2^{k+1} \rfloor$ segments S_i of consecutive elements, each of size 2^{k+1}. Since N is not divisible by 2^{k+1}, the last segment has less elements. More precisely S_t consists of the last $r := N \bmod 2^{k+1}$ elements in $\mathbb{Z}_N$. Observing that for $1 \leq i \leq t-1$, $\sum_{z \in S_i} B_k(z) = 0$, we obtain

$$\mathrm{bias}_{B_k}(N) = \left| \sum_{z \in \mathbb{Z}_N} B_k(z) \right| = \left| \sum_{i=1}^{t} \sum_{z \in S_i} B_k(z) \right| = \left| \sum_{z \in S_t} B_k(z) \right| = \left| \sum_{z=0}^{r-1} B_k(z) \right| .$$

The last term evaluates to r, if $r \leq 2^k$, and to $2^{k+1} - r$, otherwise. □

Corollary A.4 *$B_k : \mathbb{Z}_N \to \{-1, 1\}$ is unbiased if $k = k(N) = o(\log N)$.*

From equations (A.4) and (A.6), we conclude that, for odd N, $B_k : \mathbb{Z}_N \to \{-1, 1\}$ is strongly semilinear of length 2^k. This implies that $EXP_{B_k}(N, d) \leq 2^{k+1} \log(N/d)$. However, by a more tedious computation we can achieve a stronger bound for every bit B_k:

Lemma A.5 *For odd N, $EXP_{B_k}(N, d) \leq 3 bias_{B_k}(N) \log(N/d)$.*

PROOF. By definition,

$$EXP_B(N, d) = \frac{d}{N} \cdot \sum_{a \in \mathbb{Z}^*_{N/d}} |\langle B, E_{ad} \rangle| \quad .$$

Let $b_{r_k}(t)$ and T be defined as in Eq. (A.5). By the characterizations of Eq. (A.4) and Eq. (A.6) we can continue with

$$= \frac{d}{N} \sum_{a \in \mathbb{Z}^*_{N/d}} \left| \sum_{t=0}^{2^k - 1} \left(\sum_{z=0}^{b_{r_k}(t+2^k)} E_{ad}(2^k + 2^{k+1} z + t) - \sum_{z=0}^{b_{r_k}(t)} E_{ad}(+2^{k+1} z + t) \right) \right|$$

$$\leq \frac{d}{N} \cdot \sum_{a \in \mathbb{Z}^*_{N/d}} \left| \sum_{t=0}^{2^k - 1} \sum_{z=0}^{b_{r_k}(t+2^k)} E_{ad}(2^k + 2^{k+1} z + t) \right|$$

$$+ \frac{d}{N} \cdot \sum_{a \in \mathbb{Z}^*_{N/d}} \left| \sum_{t=0}^{2^k - 1} \sum_{z=0}^{b_{r_k}(t)} E_{ad}(2^{k+1} z + t) \right| \quad .$$

We will show the bound

$$\frac{d}{N} \cdot \sum_{a \in Z^*_{N/d}} \left| \sum_{t=0}^{2^k - 1} \sum_{z=0}^{b_{r_k}(t)} E_{ad}(2^{k+1} z + t) \right| \leq \frac{3}{2} \mathrm{bias}_{B_k}(N) \log \frac{N}{d}$$

on the second term. The bound on the first term can be derived analogously. Put

$$L(a,d) = \sum_{t=0}^{2^k-1} \sum_{z=0}^{b_{r_k}(t)} E_{ad}(2^{k+1}z + t) \ . \tag{A.7}$$

Recall that, by (A.5), $b_{r_k}(t) \in \{T-1, T\}$, where T is attained iff $t \leq r_k - 1$. Splitting the inner sum of $L(a,d)$ over z into two parts, where the first part ranges over all $0 \leq z \leq T-1$, and the second part over $z = T$ (what can only happen in the case of $b_{r_k}(t) = T$ which is equivalent to $t \leq r_k - 1$), we get

$$\begin{aligned}
|L(a,d)| &\leq \left| \sum_{t=0}^{2^k-1} \sum_{z=0}^{T-1} E_{ad}(2^{k+1}z + t) \right| + \left| \sum_{t=0}^{\min\{2^k-1, r_k-1\}} E_{ad}(2^{k+1}T + t) \right| \\
&\overset{(10)}{\leq} \left| \sum_{t=0}^{2^k-1} \sum_{z=0}^{T-1} E_{ad}(2^{k+1}z + t) \right| + r_k \\
&\overset{(11)}{=} \left| \sum_{t=0}^{2^k-1} E_{ad}(t) \sum_{z=0}^{T-1} E_{ad}(2^{k+1}z) \right| + r_k \ .
\end{aligned}$$

We apply (14) twice and rewrite the latter term as

$$\left| \frac{E_{ad}(2^k) - 1}{E_{ad}(1) - 1} \right| \cdot \left| \frac{E_{ad}(2^{k+1}T) - 1}{E_{ad}(2^{k+1}) - 1} \right| + r_k \ .$$

By observing that $E_{ad}(2^{k+1}) - 1 = (E_{ad}(2^k) + 1)(E_{ad}(2^k) - 1)$ and $2^{k+1}T = N - r_k$ we get

$$= \left| \frac{E_{ad}(N - r_k) - 1}{E_{ad}(1) - 1} \cdot \frac{1}{E_{ad}(2^k) + 1} \right| + r_k \ .$$

By simple trigonometrical transformations, we can express $|E_a(z)+1|$ in terms of the cosinus:

$$|E_a(z) + 1| = |2\cos(\pi a z/N)| \ . \tag{A.8}$$

Now we use bound (A.2) and equation (A.8):

$$|L(a,d)| \leq r_k \left| \frac{1}{E_{ad}(2^k) + 1} \right| + r_k = \frac{r_k}{2|\cos(2^k \pi a d/N)|} + r_k \ . \tag{A.9}$$

We now rewrite Eq. (A.7) in an alternative fashion which leads to a second independent bound on $|L(a,d)|$.

$$
\begin{aligned}
|L(a,d)| &= \left|\sum_{t=0}^{2^k-1}\sum_{z=0}^{T} E_{ad}(2^{k+1}z+t) - \sum_{t=\min\{r_k,2^k\}}^{2^k-1} E_{ad}(2^{k+1}T+t)\right| \\
&\le \left|\sum_{t=0}^{2^k-1}\sum_{z=0}^{T} E_{ad}(2^{k+1}z+t)\right| + 2^k - \min\{r_k, 2^k\} \\
&\le \left|\sum_{t=0}^{2^k-1}\sum_{z=0}^{T} E_{ad}(2^{k+1}z+t)\right| + 2^{k+1} - r_k \quad .
\end{aligned}
$$

Following along the lines of the proof above (we omit the straightforward but tedious calculation), we obtain

$$
\le \frac{2^{k+1}-r_k}{2|\cos(2^k\pi ad/N)|} + 2^{k+1} - r_k \quad . \tag{A.10}
$$

By Lemma A.3 we know that the bias of B_k equals to $\min\{r_k, 2^{k+1}-r_k\}$. Since both bounds (A.9) and (A.10) on $|L(a,d)|$ hold independently from each other this leads to the bound

$$
|L(a,d)| \le \frac{\mathrm{bias}_{B_k}(N)}{2|\cos(2^k\pi ad/N)|} + \mathrm{bias}_{B_k}(N) \le \frac{3\mathrm{bias}_{B_k}(N)}{2|\cos(2^k\pi ad/N)|} \quad .
$$

Summing the terms $|L(a,d)|$ up over all $a \in \mathbb{Z}^*_{N/d}$ we get

$$
\frac{d}{N} \cdot \sum_{a\in\mathbb{Z}^*_{N/d}} |L(a,d)| \le \frac{3d\mathrm{bias}_{B_k}(N)}{2N} \cdot \sum_{a\in\mathbb{Z}^*_{N/d}} \frac{1}{|\cos(2^k\pi ad/N)|} \quad .
$$

Since N is odd, the element 2^{-1} exists in $\mathbb{Z}^*_N$ and hence also in $\mathbb{Z}^*_{N/d}$. Substituting $a = 2^{-k}b$ we get

$$
\begin{aligned}
&\le \frac{3d\mathrm{bias}_{B_k}(N)}{2N} \cdot \sum_{b\in\mathbb{Z}^*_{N/d}} \frac{1}{|\cos(\pi bd/N)|} \\
&\le \frac{3d\mathrm{bias}_{B_k}(N)}{2N} 2\int_1^{(N/d-1)/2} \frac{1}{\cos(\pi bd/N)} db \\
&\le \frac{3d\mathrm{bias}_{B_k}(N)}{N} \int_1^{(N/d-1)/2} \frac{1}{\cos(\pi bd/N)\sin(\pi bd/N)} \\
&= \frac{3\mathrm{bias}_{B_k}(N)}{\pi}\left(\ln(\tan(\frac{\pi}{2} - \frac{\pi d}{2N})) - \ln(\tan(\frac{\pi d}{N}))\right) \\
&\le \frac{3\mathrm{bias}_{B_k}(N)}{\pi} 2\ln(\frac{2N}{\pi d}) \le \frac{3}{2}\mathrm{bias}_{B_k}(N) \log\frac{N}{d} \quad .
\end{aligned}
$$

□

Corollary A.6 *For odd N and unbiased B_k we have $EXP_{B_k}(N,d) = N^{o(1)}$ and hence B_k is balanced.*

In view of the results of the last paragraph, one may raise the question whether for a prime modulus every unbiased Boolean function necessarily is smooth. However, it is not hard to show that the ± 1 valued Boolean function B representing the Legendre Symbol is "far from being smooth", though it is unbiased. The reason for the large value of the term $EXP_B(N,k)$ is the multiplicative property of the Legendre Symbol. Since, for instance, the discrete multiplication $M(x,y) = xy$ also has a multiplicative property, $M(x,y) = xy = M(x,1)M(1,y)$, this implies that the matrix $B \circ M$ is completely determined by its first row and column:

$$B \circ H(x,y) = B \circ H(x,1) \cdot B \circ H(1,y).$$

Hence $B \circ H$ has rank one and, by Eq. (4), $\|B \circ H\|_2 = N$. Since the Legendre Symbol B is clearly unbiased we conclude from Theorem 3.4 that it cannot be smooth. A simple computation shows that $EXP_B(N,1) \approx \sqrt{N}$.

Similar considerations show that for even N the least significant bit B_0 is not smooth. More precisely, it can be shown that $EXP_{B_0}(N,N/2) = N/2$.